(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 February 2004 (12.02.2004)

PCT

(10) International Publication Number
WO 2004/014024 A2

(51) International Patent Classification[7]: H04L 12/28

(21) International Application Number:
PCT/US2003/024180

(22) International Filing Date: 31 July 2003 (31.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/211,841 2 August 2002 (02.08.2002) US

(71) Applicant: **WAVELINK CORPORATION** [US/US]; 11332 NE 122nd Way, Suite 300, Kirkland, WA 98034 (US).

(72) Inventors: **WHELAN, Robert**; 545 Kirkland Avenue, Kirkland, WA 98033 (US). **VAN WAGENEN, Lamar**; 980 E. Diana Hills Way, Sandy, UT 84094 (US). **MORRIS, Roy**; 8812 NE 191st Place, Bothell, WA 98011 (US).

(74) Agents: **LEBOWITZ, Henry, C.** et al.; Pennie & Edmonds LLP, 1155 Avenue of the Americas, New York, NY 10036 (US).

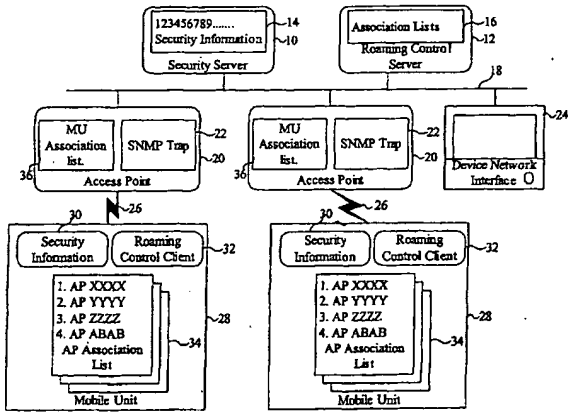
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: MANAGED ROAMING FOR WLANS



System Diagram

(57) Abstract: The present invention allows any number of mobile units to roam between a large numbers of sub-networks, each with a large number of access points (tens of thousands or more total access points), with minimal direct administration effort. A hierarchy of management servers may be used across the multiple sub-networks, which can be under the control of multiple entities. The invention provides the capability for the mobile units to authenticate the access points associated with, to ensure they are both authorized and managed. Peer-to-peer and ad hoc associations between mobile units are managed as welt. The invention may enforce a number of association policies such as, for example, forcing the mobile unit to only associate with access points or mobile units on a previously set mandatory association list, providing the mobile unit with a list of preferred access points to associate with, but allowing association with other access points, or providing the mobile unit with a excluded association list of access points or mobile units it is not to associate with.

WO 2004/014024 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

U.S. Express Mail No: EL 477 037 572 US
Attorney Docket No. 10629-0033-999

MANAGED ROAMING FOR WLANS

FIELD OF THE INVENTION

The present invention relates to the management of mobile unit roaming on Wireless Local Area Networks (WLAN). More specifically, the invention relates to a system to aid in network management and to enhance network security by controlling policy for the associations between mobile units and known and managed access points.

BACKGROUND OF THE INVENTION

WLANs are now in common use in both large and small businesses, as public Internet access points, and in home environments. Millions of access points and mobile units are now deployed. Enterprises commonly deploy wireless access points on one or more sub-networks often at multiple geographic locations. There is a growing trend toward employing WLAN technology for public Internet access points used by travelers or other mobile users. In a WLAN, one or more base stations or Access Points (AP) bridge between a wired network and radio frequency or infrared connections to one or more mobile stations or Mobile Units (MU). The MUs can be any of a wide variety of devices including, laptop computers, personal digital assistants, wireless bar code scanners, wireless point of sale systems or payment terminals, and many other specialized devices. Most WLAN systems used in business and public access environments adhere to one or more of the IEEE 802.11 family of specifications.

Since access points use a simple bridging protocol they can be added to any wired protocol compatible network without any centralized control or intervention and once added are difficult to detect. For example, an IEEE 802.11 compliant access point can be made operational by simply connecting it to a wired Ethernet and applying power. In some cases well-intentioned individuals, who do not realize the potential problems they may be creating, add unauthorized access points to wired LANS. In other cases, a malicious attacker or hacker adds the access point to the

wired LAN to gain unauthorized access. These unauthorized and unmanaged access points are known as rouge access points. In yet other cases, an access point on another network or sub-network associates with an organization's mobile units. These cases can include situations were a hacker attempts to deliberately spoof the mobile units into associating with a malicious access point. Unauthorized access points attached to other networks are referred to as foreign access points. To prevent these problems, a means is required to allow network administrators to control which access points a mobile unit associates with.

Present IEEE 802.11 WLAN standards are designed to facilitate the roaming of mobile units between multiple access points, which may be connected to one or more wired LANs. As a mobile unit travels from the coverage area of one access point to another it will associate with the new access points using the Extended Service Set (ESS) protocols. The new access point the mobile unit associates with can be on the same sub-network or another sub-network. The standard IEEE 802.11 protocols provide no capabilities for external management of the roaming process. In addition, the IEEE 802.11 standards provide no means for a mobile unit to authenticate an access point.

Several methods including the RADIUS protocols and the Extensible Authentication Protocol (EAP, RFC 2284) provide capabilities to authenticate end-to-end connections. Likewise, Virtual Private Networks (VPN) create secure tunnels through public networks. A related scheme using a proxy server and address translation is disclosed in EP 11113641 to Moles and Herle. None of these protocols allows a mobile unit to determine if it is connected to the desired access point and therefore the correct network or sub-network.

Mobile unit radio drivers typically provide the capabilities to set a preferred Basic Service Set Identifier (BSSID) or exclusive BSSID. In practice, the BSSID is equal to the MAC address of the access point for the association. Thus, the radio drivers provide the ability to instruct the mobile unit to prefer a particular single access point association or to exclusively use a particular single access point association. This limited capability does not allow for the external management of

the multiple access point associations possible for a roaming mobile unit, and supported by the ESS protocols.

Access control lists are commonly used to manage the access of users and client programs to network services and data. Numerous examples of access control list management environments can be found include, those sold by Baltimore Technologies, IBM's Tivoli Division, and the capabilities built into Microsoft's Windows 2000 operating system. Yet none of these technologies provides the ability to manage the dynamic roaming and access point associations required in a WLAN environment. Further, these technologies do not provide a means for the mobile unit to authenticate the access point or any other common network infrastructure.

Other prior art describes various schemes to facilitate the handoffs between access points when a mobile unit roams. Yet none of these systems address the management or authentication of the associations between the mobile units and the access points. Examples of such systems are disclosed in WO 0215472 to Singhal, et. al., US 5594731 to Reissner, US 3212806 to Natarajan, and US 6188681 to Vesuna

Several schemes have been proposed to provide for mutual authentication between access points and mobile units. Two such schemes are disclosed in EP 1178644 to Jorma, et. al., and US 20001 0048744 to Kimura. Both of these schemes assume that each access point and each mobile unit has access to the required security keys. Further, these schemes assume that suitable modifications can be made to the access points to accommodate these protocols.

SUMMARY OF THE INVENTION

In one aspect the present invention comprises a system for securely accessing a wireless network, further comprising a wireless mobile device configured to use wireless network protocols conforming to one or more of the IEEE 802.11 family of specifications; a program executing on the wireless mobile device; the program being configured to cause the mobile device to use an association control list to control communication with access points; the association control list

comprising a plurality of BSSIDs; the program being further configured to update the association control list by communicating with a server.

In another aspect, the invention comprises a system for securely accessing a wireless network, further comprising a wireless mobile device; a program executing on the wireless mobile device; the program being configured to cause the mobile device to use an association control list to control communication with access points; the association control list comprising digital data representing information concerning at least one access point and whether the wireless mobile unit should communicate with the at least one access point.

In still another aspect, the present invention comprises a system for securely accessing a wireless network, further comprising: a wireless mobile device comprising a processor and memory; a program executing on the wireless mobile device; the program being configured to cause the wireless mobile device to associate with an access point and to send a request to a server for confirmation that the access point is authorized; the access point comprising a wireless device for communicating with wireless devices and a wired network interface for communicating via a wired network.

In still another aspect, the invention comprises a system for securely accessing a wireless network, further comprising: a server configured to receive a request to authenticate an access point from a wireless mobile device; the server being further configured to determine whether the wireless mobile device is associated with the access point and whether the access point is authorized, and to provide a response to the wireless mobile device indicating whether the mobile device is authorized to continue association with the access point.

In another aspect, the invention comprises a wireless communication security system, further comprising: a first wireless mobile device; a program executing on the first wireless mobile device; the program being configured to cause the first wireless mobile device to use an association control list to control communication with other wireless mobile devices; the association control list comprising a plurality of identifiers, each identifier uniquely identifying a wireless mobile device.

In another aspect, the invention comprises a system for securely accessing a wireless network, further comprising a wireless mobile device; a program executing on the wireless mobile device; the program being configured to cause the mobile device to use an association control list to control communication with access points and to update the association control list by communicating with a server.

In yet another aspect, the system comprises a system for securely accessing a wireless network, comprising a server system comprising at least one server computer and at least one software program executing on the at least one server computer; the at least one server computer being operatively connected to a communications network; the system being configured to receive at least one access point identifier from a wireless mobile unit; the system being further configured to transmit to the wireless mobile unit information concerning at least one access point and whether the mobile unit should communicate with the at least one access point.

In another aspect, the invention comprises a system for securely accessing a wireless network, further comprising an access point comprising a wireless device for communicating with wireless devices and a wired network interface for communicating via a wired network; the access point being configured to wirelessly transmit an association control list; the association control list comprising digital data representing information concerning at least one access point and whether at least one wireless mobile unit should communicate with the at least one access point.

In another aspect, the invention comprises a system for securely accessing a wireless network, further comprising a wireless mobile unit comprising a processor and memory; a program executing on the wireless unit, the program being configured to cause the wireless mobile unit to transmit to a server system a data structure comprising identifiers of access points within range of the wireless mobile units; the program being further configured to receive from the server system information concerning at least one access point and whether the mobile unit should communicate with the at least one access point.

In still another aspect, the invention comprises a system for securely accessing a wireless network, further comprising: a wireless mobile unit comprising

a processor and memory; a program executing on the wireless unit, the program being configured to cause the wireless mobile unit to receive an association control list from an access point; the association control list comprising digital data representing information concerning at least one access point and whether the wireless mobile unit should communicate with the at least one access point.

The foregoing statements of the features of the invention are not intended as exhaustive or limiting, and the proper scope of the invention is to be understood with reference to this entire disclosure and to the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described by reference to the preferred and alternative embodiments thereof in conjunction with the drawings in which:

Fig. 1 is an overall schematic diagrammatic view according to one embodiment of the invention:

Fig. 2A, Fig. 2B, and Fig. 2C is a process flow diagram according to one embodiment of the invention; and,

Fig. 3 is an overall schematic diagrammatic view according to another embodiment of the invention

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The following detailed description refers to the accompanying drawings and describes exemplary embodiments of the present invention. Other embodiments are possible and modifications may be made to the exemplary embodiments without departing from the spirit, functionality and scope of the invention. Therefore, the following detailed descriptions are not meant to limit the invention.

The invention provides the capability for the mobile units to authenticate the access points with which they associate with, to ensure they are authorized and/or managed. In addition, the system can enforce a number of association policies including:

(a) forcing the mobile unit to only associate with access points on a previously set mandatory association list;

(b) providing the mobile unit with a list of preferred access points to associate with, but allowing association with other access points; and,

(c) providing the mobile unit with an excluded association list of access points it is not to associate with.

The invention manages the access point associations of mobile units through the distribution and management of association lists from one or more management servers to management clients on the one or more mobile units. The lists can contain mobile unit identifiers (preferably BSSIDs) for access points with which the mobile unit must exclusively associate, the BSSIDs for access points the mobile unit preferentially associates with, and identifiers for access points with which the mobile unit is excluded from associating. Mobile units using mandatory association lists will typically not need to maintain preferred association lists or excluded association lists. Typically, mobile units using mandatory association lists are used in a restricted environment where network managers want to limit the roaming of the mobile unit. Mobile units maintaining preferred association lists can, optionally, maintain excluded association lists or vise versa. Mobile units using preferred association lists and excluded association lists are free to roam to any access point (except the excluded ones), as required, but will use the preferred access points (if available).

When a mobile unit roams to an access point on a new sub-network it can optionally perform a login procedure with a security server, during which authentication information, such as shared secret information, is typically exchanged. At the same time the mobile unit typically verifies the access point being used through the security server to verify that it is in fact a known and managed access point. The login procedure provides verification to the security manager that the mobile unit is an authorized one. The verification of the access point demonstrates it is the authorized access point and not another access point spoofing the legitimate authorized access point. As the mobile unit roams from one access point to another within the same sub-network, the security server preferably verifies each access point with which the mobile unit associates to ensure that the mobile unit is not being spoofed.

The invention allows management of mobile unit associations with numerous access points attached to a large number of wired sub-networks. Many existing access points do not have the flexibility to manage large association lists or to directly perform authentication protocols with the mobile units. Further, it may be impractical in some organizations to create and distribute a single association list for all access points. When a mobile unit, using a preferred association list, first connects to a new sub-network, possibly in a new geographic location, it determines which access points have sufficient signal strength to associate with. The mobile unit looks in the preferred association list to determine if any of the access points are on the list, and if so initiates an association with them. If none of the access points are on the preferred association list the mobile unit checks the excluded association list (if any) to verify that it can associate with one or more of the access points. The mobile unit then associates with any one of the allowed access points on a temporary basis. Once an association is made, the mobile unit generally logs into a security server and authenticates the access point. The mobile unit then connects to a management server and down loads the preferred association list for that sub-network. The mobile unit can maintain the current association if the access point being used is on the preferred association list. If not, the mobile unit will attempt to discover and associate with an access point on the preferred association list, as part of normal operation.

The invention provides the capability for mobile units to use the services of multiple security servers and roaming management servers under control of one or more organizations. Each set of servers can manage one or more sets of association lists for the access points under control of these organizations. The lists can be organized in a hierarchical manner. In one example, an organization may have the top level of the hierarchy controlled by the servers at the headquarters, and with servers on sub-networks in departments or at regional offices controlling lower levels of the hierarchy. The hierarchy can be further organized to manage network traffic, network access, etc., as required. The organization may choose to have access points on its own sub-network used for primary access, and those of an external service provider used for secondary access. In this way, the organization can minimize the fees paid to the service provider, while still gaining benefits of the

service. In another example, the public access point service provider uses the hierarchical association lists to require customers' mobile units to preferentially associate with the company's access points and use roaming partners' access points only when one of the company's own access points is not accessible.

In cases where a mobile unit is using a mandatory association list and must connect to a new sub-network the invention provides a secure wired list update or synchronization capability. The mobile unit connects to the wired network, and optionally authenticates with a security server. A management server then loads a new or updated exclusive association list into the mobile unit. Using this new list, the mobile unit can begin communications with any access points on the list. Mobile units using preferred access lists or exclusion lists can use the same wired update and synchronization capability if they are unable to update those lists over the wireless network.

Since new access points can be added to any of the wired sub-networks at any time, the management server attempts to auto-discover the presence of the new access points. Typically, the management server auto-discovers a new access point by detecting its MAC address through monitoring of layer 2 packet headers or by monitoring inter-access point communications. Once a new access point is auto-discovered, the management server adds it to the appropriate mobile unit access management lists. A network management server may then automatically configure the access point to reflect the organization's network management policies and procedures. Generally, only access points that can be profiled and managed are added to the access lists. Access points that are of unknown or unmanageable types are typically added to the excluded list. At the same time the security server will enforce security policies for the newly discovered access points and will subsequently be able to authenticate the association of mobile units with the new access points. As an added security and network administration measure, the management server may query a network administrator for approval before updating the lists. If multiple, distributed management servers are used, list updates are propagated to the other servers, as required. The update association management list is then sent to all mobile units associated with the managed access points on the sub-network.

Peer-to-peer or ad-hoc associations created between mobile units introduce particular security and network management problems. Hackers can use peer-to-peer associations to gain unauthorized access to data and networks. To address these and other problems the invention provides the capability to manage peer-to-peer associations. Peer-to-peer association policies, which can be enforced with the invention, can include but are not limited to:

(a) not allow any peer-to-peer or ad-hoc associations;

(b) only allow peer-to-peer associations between mobile units with mutual authentication capability, information on which mobile units have this capability possibly coming from a preferred association list;

(c) only allow peer-to-peer associations between mobile units on a specific mandatory association list; and,

(d) only allow peer-to-peer associations between mobile units on a specific mandatory association list, and for which mutual authentication is possible.

A diagrammatic view of one embodiment of the invention is shown in Figure 1. This discussion is intended to show an exemplary embodiment only. It will be understood by those skilled in the art that the functional blocks shown on the diagram can be combined or further distributed as required for a given implementation without changing the function, scope or spirit of the invention.

The roaming control client **32** manages roaming of the mobile units **28** between the multiple access points **20** on one or more sub-networks **18** through the wireless links **26**. The roaming control client uses the one or more AP association lists **34** to determine mandatory access point associations, preferred access point associations and excluded access point associations.

When mobile units **28** roam to new sub-networks **18** or are initialized, one or more security servers **10** authenticate the mobile units **28**, typically using security information stored by the server **14** and in the mobile unit **30**. The security server also provides a means for the mobile units to authenticate associations with access points **20**, typically using Simple Network Management Protocol (SNMP) traps **22** and MU association lists **36**.

The roaming server **12** creates and maintains association lists **16** which are distributed to the mobile units **28** for storage **34**. The roaming control client **32** on the mobile unit **28** uses these one or more association lists to manage the roaming of the mobile unit between access points **20** on one or more sub-networks **18**. A mobile unit can receive a set of hierarchically organized lists from multiple roaming control servers, which are, themselves, hierarchically organized and possibly under control of different organizations.

The one or more sub-networks **18** are typically interconnected and provide connectivity between one or more security servers **10**, one or more roaming control servers **12**, the mobile units **28**, and the access points **20**. The security servers and roaming servers are organized hierarchically and a server can be used on one or more sub-networks. Control or administration of the servers typically falls to the organization controlling the sub-networks managed. In some embodiments the roaming control servers and/or security servers can be distributed to execute in whole or in part on the access points **20**. In some embodiments, the association lists are created on one or more centralized or distributed roaming control servers, and stored on the access points, from which, the lists are distributed to the mobile units.

When a mobile unit **20** requires synchronization of the access point association lists **34** or shared secret keys **30** through the wired network **18**, the mobile unit is connected to the network device interface **24**. Once connected to the network device interface the mobile unit can directly communicate to the one or more roaming servers **12** and one or more security servers **10**. The network device interface can be of any suitable type including, a network interface card for direct cable connection or a cradle.

Preferred Association List Process Flow

Mobile units **28** can connect to or roam to one or more sub-networks **18** where they associate with one or more access points **20** under control of the roaming control client **32**. Once a mobile unit has associated with an access point, it can roam to other access points on the same sub-network or roam to another sub-network. A process flow diagram for a mobile unit using a preferred association list

34 and an optional excluded association list 34 is shown in Figure 2A, 2B, and 2C. This discussion is intended to be an exemplary embodiment only. It will be understood by those skilled in the art that the order the steps described can be changed, certain steps can be removed and new steps added without changing, the scope, spirit or functionality of the invention.

A mobile unit 28 initiates an association process 50 to an access point 20 on a sub-network 18 either when it is initialized or roams to the new sub-network. The mobile unit detects available access points 51, typically using the methods specified in the IEEE 802.11 specifications. Based on the sub-network identification (or ESSID) the roaming control client invokes 52 the correct set of association control lists 34. The roaming control client on the mobile unit determines 54 if any of the detected access points are on its preferred association list 34. If one or more of the access points is on the preferred list, the mobile unit will associate with the preferred access point 55. The security server 10 then optionally authenticates the mobile unit 60. The mobile unit may optionally authenticate 62 the access point, possibly using the assistance of the security server. The mobile unit can then begin regular communications 76.

If none of the access points 20 is on the preferred list, the roaming control client 32 in the mobile unit 28 determines 58 if a given access point is on the excluded list 34. If not, the roaming control client creates a temporary association 56 with the best available access point. The security server 10 then optionally authenticates the mobile unit 60. The mobile unit may optionally authenticate 62 the access point 20, possibly using the assistance of the security server. The mobile unit can then begin regular communications 76.

If the access point 20 the mobile unit 28 is associated with is on the excluded association list, the roaming control client determines if there is another usable access point 66. If so, the roaming control client determines if the access point is on the excluded association list 58. If all available access points 20are on the excluded association list 34, the roaming control client 32 indicates to the user of the mobile unit 28 that an association cannot be made. The user is given the option to synchronize the association lists on the wired network 18. The user then determines

if this connection is possible **59**. If not, the mobile unit continues to detect access points **51** until a usable one is discovered. If a wired network connection is possible, the user connects **68** the mobile unit to any available network device interface **24**. The security server **10** then optionally authenticates **70** either the user or the mobile unit itself or both. Suitable authentication methods are discussed in a section below. If required, security information **14** on the security server **10** is exchanged to update the security information on the mobile unit **30** at this time. Once authenticated, the roaming control client on the roaming control client polls the roaming server **12** and determines if the association lists on the mobile unit **34** needs to be synchronized with the lists **16** on the server, and if so, updates the association lists **71**. In an alternative embodiment, the roaming control server discovers the presence of the mobile unit at the network device interface and initiates the synchronization of the association control lists. Once the association lists on the mobile unit are synchronized, the mobile unit attempts to detect access points **51** and continues the process already described.

If no access point on the preferred list can be located the mobile unit **28** initiates a temporary access point **20** association **56,** the roaming control client **32** discovers which roaming control server **12** and security server **10** to use on that sub-network **18** and optionally authenticates the servers **57**. The security server then, optionally, authenticates **60** the mobile unit using the security information **14, 30**. Suitable authentication methods are discussed in a section below. The mobile unit then optionally authenticates the association with the access point **62**. The mobile unit then begins regular communications **76** through the sub-network **18** and beyond.

When a mobile unit **28** associates with a new sub-network **18** it discovers the security server **10** and roaming control server **12** with authority for that sub-network. The servers identify themselves to the mobile unit by a server identifier (server ID). This discovery process can use any suitable method, including:

(a) broadcasting a message to solicit a response from the servers indicating the server ID, followed by mutual authentication between the mobile unit and the servers;

(b) contacts the correct server for the sub-network (determined by the sub-

network address) by a fixed or preset network (IP) address, typically followed by mutual authentication between the mobile unit and the servers; and,

(c) connecting to central servers (typically at a fixed network address), which return the addresses for the servers used on that sub-network and, typically followed by mutual authentication between the mobile unit and the servers.

Once communications with the sub-network **18** and beyond have been established **76**, the roaming control client **32** begins a regular process of roaming management. This process proceeds in an infinite loop until the mobile unit **28** is turned off or reinitialized.

The roaming control client **32** determines if the mobile unit **28** is roaming **78** to a new access point **20**. If so the mobile unit detects the presence of other access points **80.** The roaming control client determines **82** if the new access points are on a new sub-network **18.** If so the access point invokes the correct association control lists for that sub-network **84.**In either case, the roaming control client determines **54** if any of the access points detected are on the preferred association list **34.** The process then proceeds as has already been described.

Periodically, the roaming control client **32** determines **92** if the mobile unit **28** is associated with an access point **20** on the preferred association list **34.** If not, the mobile unit attempts to detect **94** an access point on the preferred association list. If a suitable access point can be found **96,** the mobile unit associates with it **98.** The roaming control client can then, optionally, authenticate the access point **100,** using any suitable method as is described below.

If the roaming control server **12** has a new or updated association list **16** or lists available **102,** the roaming control client **32** synchronizes **104** the updated list(s) to the mobile unit **28.** The roaming control client periodically polls the roaming control server to determine if a new or update list is available. Alternatively, the roaming control server can notify the roaming control clients on the mobile units associated with the one or more sub-networks **18** whenever a new or updated list is available.

Use of Mandatory Association Lists

In situations where maximum security is required or where network administrators wish to limit the roaming of mobile units **28** for some other reason, a mandatory association list **34** is employed. When a mandatory association list is employed the roaming control client **32** forces the mobile unit to only associate with access points **20** that are on the list. In some embodiments, the roaming control client selects the correct association list based on the identifiers for the sub-network. Whenever a mobile unit **20** using a mandatory association list **34** is initialized or roams to a new sub-network it typically executes the following steps:

(a) the roaming control client **32** in the mobile unit **28** detects the presence of any access points **20** using standard IEEE 802.11 protocols;

(b) the roaming control client looks on the mandatory association list **34** to determine if any of the available access points are on that list; and,

(c) the mobile unit associates with one of the access points on the mandatory association list; and,

(d) optionally, the security server **10** authenticates the mobile unit and the mobile unit authenticates the access point using the methods described latter in this document.

If none of the available access points 20 are on the mandatory association list **34**, the list may need to be synchronized or updated on the wired network **18**. The mobile unit may inform the user of the need to synchronize the list. The user connects **68** the mobile unit to any available network device interface **24**. The security server **10** then optionally authenticates either the user or the mobile unit itself or both. Suitable authentication methods are discussed in a section below. If required, security information on the security server **14** is exchanged to update the security information on the mobile unit **30** at this time. Once authenticated, the roaming control client on the mobile unit **28** polls the roaming control server **12** and determines if the association lists **34** on the mobile unit needs to be synchronized with the lists **16** on the server, and if so, updates the lists. In an alternative embodiment, the roaming server discovers the presence of the mobile unit at the network device interface and initiates the update. Once the mandatory association

list on the mobile unit is updated, the mobile unit associates with one of the access points on the list and optionally authenticates the access point.

When the mobile unit **28** must roam to another access point **20**, the roaming control client **32** typically executes the following steps:

(a) the roaming control client **32** in the mobile unit **28** detects the presence of any access points **20** using standard IEEE 802.11 protocols;

(b) the roaming control client looks on the mandatory association list **34** to determine if any of the available access points are on that list; and,

(c) the mobile unit associates with one of the access points on the mandatory association list; and,

(d) optionally, the mobile unit authenticates the access point using the methods described latter in this document.

Mobile Unit Authentication

The one or more security servers **10** can perform the authentication of the mobile unit **28** through any suitable method. In general a cryptographic authentication is preferred. Those skilled in the art will be familiar with multiple suitable methods.

In one embodiment, the security information **14, 30** on the security server **10** and the mobile unit **28** is a shared secret key. In this case messages with known content are typically exchanged between the security server and the roaming control client **32.** If these messages can be decrypted satisfactorily, the server and the mobile unit have successfully authenticated each other. This authentication can be symmetric (as just described) or asymmetric where only the mobile unit is authenticated.

In another embodiment, the security information **14, 30** on the security server **10** and the mobile unit **28** is a Public Key Infrastructure (PKI) certificate. In this case the security server can act as the PKI certificate authority or certification authority. Alternatively. the security server can use an external certificate authority or certification authority. The authentication, once again, can be symmetric or asymmetric.

As an alternative or supplement to authentication of the mobile unit **28**, the user can be authenticated. The security server **10** typically performs this authentication using the security information **14, 30**. This authentication can be a simple user name and password login, preferably using an encrypted connection (i.e. SSL). Alternatively a cryptographic method can use techniques including PKI or shared factor authentication protocols such as Keberos.

In some embodiments, the security server **10** allows the mobile unit **28** a certain period of time to complete the authentication process. If the mobile unit cannot complete the authentication process within the prescribed period of time, the security service will consider the mobile unit to not be authenticatable. Alternatively, a mobile unit, which cannot execute the authentication protocol correctly, is considered not to be authenticatable. Access for none authenticatable mobile units can be restricted in any manner desired. Some examples of access restrictions include:

(a) The security server **10** can instruct the access points **20** to cease association with the non-authenticatable mobile unit **28**, effectively preventing the mobile unit from obtaining access to the network **18**;

(b) The security server **10** can connect the mobile unit **28** to the network **18**, through the access points **20**, using a restricted access virtual LAN. The virtual LAN may give the user of the mobile unit access to public services, including the Internet, but not internal services, as a guest user; and

(c) The security server can allow connection of the mobile unit **28** to the network **18**, through the access points **20**, while limiting network services access using an access control list or other means.

In every case the security information **14, 30** on the security server **10** and the mobile unit **28** are preferably exchanged on a wired sub-network **18**, using the device network interface **24**, to improve security. Alternatively, the security information can be exchanged or updated over the wireless connection **26**.

Access Point Authentication

To prevent spoofing attacks by foreign access points, the mobile unit **28** will

usually authenticate any access points **20** it associates with. Access points do not typically have built in authentication capability. Still a number of suitable methods exist for this authentication. Generally, the mobile unit uses the services of the security server **10**.

In one embodiment, the security server **10** subscribes to the messages from an SNMP trap **22** on the access point **20**. When a mobile unit **28** associates with that access point, the trap sends a message indicating the association information. The roaming control client **32** on the mobile unit polls the security server, which verifies (or not) that it has received the message for that association. In an alternative embodiment, the security server transmits a authentication message to the roaming control client as soon as the SNMP message is received.

In another embodiment, the roaming control client **32** on the mobile unit **28**, polls the security server **10**, which in turn, polls the access point **20** to receive the MU association list **36**. The security server verifies that the mobile unit association is on the list (or not) and reports the result to the roaming control client.

Management of Peer-To-Peer Associations

Peer-to-peer associations between mobile units **28** are manage by the roaming control client **32** using the security information **30** and association lists **34**. These association lists are synchronized with the one or more roaming control servers **12** as has already been described. The roaming control clients can execute a number of peer-to-peer association policies, which can include but are not limited to:

(a) not allow any peer-to-peer or ad-hoc associations;

(b) only allow peer-to-peer associations between mobile units with mutual authentication capability, information on which mobile units have this capability possibly coming from a preferred association list;

(c) only allow peer-to-peer associations between mobile units on a specific mandatory association list; and,

(d) only allow peer-to-peer associations between mobile units on a specific mandatory association list, and for which mutual authentication is possible.

The mobile units can perform mutual authentication during peer-to-peer associations in a number of suitable ways. Suitable techniques include:

(a) the mobile units exchange messages encrypted with a shared secret key or use a shared factor authentication protocol such as Keberos;

(b) the mobile units are authenticated through the security server **10**, and the security server sends authentication messages to the mobile units participating in the association; and,

(c) authentication through an external certificate authority or certification authority, possibly using PKI techniques.

Hierarchical Roaming Management

In many practical situations, multiple security servers **10** and/or multiple roaming control servers **12** will be used. The invention provides the capability to manage these multiple servers in a hierarchical structure. Generally, this hierarchy is organized with respect to a mobile unit **28** or a group of mobile units belonging to a particular organization. In other words, each organization with management responsibility for management of mobile units will create and manage a hierarchy suitable for its association policies. Typically, an organization will make one set of servers, under its control, the top of the hierarchy for the mobile units under its control. Both the roaming control servers and the security servers can manage mobile unit **28** associations on one or more sub-networks **18**. For example, a company may choose to make the servers at the headquarters the top of the hierarchy with servers in departments and other sub-networks or geographic locations organized into a tree structure. In another example, a company may choose to use external service providers for wireless network access, and may therefore choose to make its own servers the root of the hierarchy with the service provider's servers as subservient.

The security information **14** in the hierarchy of security servers **10** and the association lists **16** in the roaming control servers **12** can be propagated to the other servers by any suitable methods. Two examples of such methods are:

(a) servers synchronize security information and association lists both up and down the hierarchy so that common information is held by all servers; and,

(b) servers act as proxy servers for others up and down the hierarchy and thus do not store all information locally, but rather traverse the hierarchy to find the required information or services.

The method used to propagate the security information **14** and the association lists **16** need not be the same. In one example, the association lists are propagated to all roaming control servers **12** in the hierarchy, while security information is kept in a "home" security server **10** and is accessed by other security servers through a proxy protocol. Alternatively, each mobile unit **28** can store security information **30** for each sub-network **18** it uses. In this case, the security servers **10** for each sub-network contain the corresponding security information **14**. The servers have a server ID, used by the mobile unit to refer to the correct servers for each sub-network.

Mobile units **28** connect to the appropriate servers for the sub-network **18** they are associating with. Methods used by the mobile units to discover the correct servers have already been discussed. The mobile units maintain one or more sets of association lists **34** for the access points **20** on each sub-network it uses. The correct set of association lists can be invoked based on the sub-network address and corresponding server ID. Alternatively, the appropriate lists **16** can be dynamically loaded from the roaming control server **12**, whenever the mobile unit roams to sub-network.

Access List Management

The invention provides capabilities to reduce the workload on network managers or network administrators. These capabilities include, addition or deletion of new access points to the association lists **16** managed by the roaming control server **12**, and the addition, updating and deletion of security information **14** in the security server **10**. Updated association lists and security information is then propagated to the mobile units **20** as has already been described. Manual operations performed by network administrators are either performed on an integrated network management console or an application specific user interface.

The roaming control server **12** attempts to auto-discover the presence of the new access points **20** added to the network **18**. Typically, the roaming control server auto-discovers a new access point by detecting its MAC address through monitoring of layer 2 packet headers or by monitoring inter-access point communications. Once a new access point is auto-discovered, the roaming control server adds it to the appropriate association lists **16**. Generally, only access points that can be profiled and managed are added to the access lists. Access points that are of unknown or unmanageable types are typically added to the excluded list. At the same time, the roaming server notifies the security server **10** of the presence of the new access point. The security server then enforces security policies for the newly discovered access points and will subsequently be able to authenticate the association of mobile units with the new access points. As an added security and network administration measure, the management server may query a network administrator for approval before updating the lists. If multiple, distributed management servers are used, list updates are propagated to the other servers, as required. The update association management list is then propagated to all mobile units **28** associated with the managed access points on the sub-network **18**.

In some embodiments, the roaming control server **12** can attempt to build preferred access point **20** association lists **16, 34** based on a number of criteria, as determined by administration policies. Examples of access point association policies, which can be used or combined arbitrarily, may include but are not restricted to:

(a) Access points **20** with better management capability;

(b) The level of security capability in the access point **20**, with preference given to access points able to execute the security protocols best suited to the applications software being run on each particular mobile unit **28**;

(c) The quality of service capabilities or capacity of the access point **20** and the network **18** connected to the access point. For example, mobile units **28** running applications requiring high bandwidth or fast response times may prefer to use higher capacity or faster access points, while access points with lower bandwidth or longer response times can be used by mobile units with less critical applications; or

(d) The cost of using a particular access point **20**, with preference given to the least expensive association with suitable characteristics to run the applications or services required by each mobile unit **28**.

In some embodiments, users of mobile units **28** can configure the association control lists **34**. This configuration is allowed provided it does not violate any policy or setting configured by the one or more roaming control servers **12**.

Alternative Association List Distribution

In some alternative embodiments, the association control lists **16**, **34** are broadcast, on the wireless links **26**, by the access points **20** to the mobile units **28** on a periodic basis. This broadcast may be a part of the beacon message access points periodically transmit or may be a separate broadcast. When a mobile unit wishes to associate with access points on a sub-network **18**, it receives the association control list in the broadcasts from the one or more access points on the sub-network. The roaming control client **32** uses the information in the lists to allow the mobile unit to associate with one or the access points. Once associated, the mobile unit may be authenticated by the security server **10** and may then authenticate the access point, possibly using the services or the security server. In one embodiment, the list is signed by a trusted party and the signature is verified by the mobile unit before relying on the list.

If the mobile unit **28** is unable to authenticate the access point **20** or verifiy a trusted signature on the association lists **34**, the association lists **34** received may not be trustworthy. The mobile unit may take one of a number of actions, including:

(a) continue the association with the unauthenticated access point while searching for association lists from an authenticatable access point;

(b) cease association with the unauthenticated access point and search for another authenticatable access point, and;

(c) limit information transmitted though the unauthenticated access point while searching for association lists from an authenticatable access point.

In many respects this alternative embodiment is similar to the embodiments already described. The only difference being the method used to distribute the

association control lists. Other details of operation can be inferred from the previous discussion.

In some alternative embodiments the association management and authentication is performed on a centralized or distributed servers rather than on the mobile units. A diagrammatic view of one of these alternative embodiments is shown in Figure 2. This discussion is intended to show an exemplary embodiment only. It will be understood by those skilled in the art that the functional blocks shown on the diagram can be combined or further distributed as required for a given implementation without changing the function, scope or spirit of the invention. Further, many of the details of other embodiments, already discussed, apply equally to the alternative embodiments.

The roaming control server **154** manages the associations of the one or more mobile units **168** with the multiple access points **160** on one or more sub-networks **158,** through the wireless links **166.** The roaming control server creates and uses the one or more association lists **156** to determine mandatory access point associations, preferred access point associations and excluded access point associations for the mobile units. These association management policies have already been described. Methods for creation and management of the association lists and policies have already been discussed.

When a mobile unit **168** is initialized or needs to connect with a new sub-network **158**, it creates a temporary association with an access point **160.** The choice of this access point is determined by criteria that are familiar to those skilled in the art, such as, Received Signal Strength Indication (RSSI) on the wireless links **166**. Once the temporary association has been made the security server **150** will optionally authenticate the mobile unit, generally through the exchange of security information **170** and comparing this information with the information stored in the server **152.** Alternatively, other security methods such as Public Key Infrastructure can be applied. In some embodiments, the security server will periodically authenticate the access points **160.** Suitable methods for the authentication of mobile units and access points have already been discussed in detail.

Once the mobile unit **168** has temporarily associated with an access point **160**, and optionally been authenticated, the roaming control client **172** sends information (including ESSID, BSSID and RSSI) to the roaming control server **154**. The roaming control server uses this information and the association control lists **156** to determine which access points **160** the mobile unit should associate with. The association information is transmitted to the roaming control client, possibly over a secure connection. The roaming control information can take the form of a mandatory command or a recommendation. Typically a recommendation is made in association with a prefer association list and a command is issued to enforce policies for excluded or mandatory association lists. Based on the information received the mobile unit takes the appropriate action, which may include:

(a) maintaining the association if the access point is on the preferred or mandatory association lists;

(b) changing association to a recommended access point, if one is available;

(c) ceasing association with an access point on an excluded list, and change association to an allow access point, if one is available; or

(d) ceasing association with an access point not on a mandatory association list and change association to an access point on the list, if one is available.

In some embodiments, the roaming control client **172** reports a new access point **160** association to the roaming control server **154**. As an added security and network management step the roaming control server can optionally verify this association with the access point. This verification can be accomplished in a number of ways including, for example, (a) verifying that the mobile unit is on the MU association list **164** or (b) receiving an Simple Network Monitoring Protocol (SNMP) trap **162** from the access point indicating the new association.

Once the mobile unit **168** and roaming control server **154** have completed and possibly verified an access point **160** association, the mobile unit begins normal communications with one ore more entities connected to the sub-network **158**, the wireless links **166**, and beyond. In cases where the mobile unit is unable to perform the association instructions, the security server **150** cannot authenticate the mobile unit or the access point, or the roaming control server **154** cannot verify the

association between the access point and the mobile unit, the to connections and services on the sub-network and beyond may be restricted. Methods to restrict network and service access have already been discussed in detail.

One or more security servers **150** and roaming control servers **154** can manage associations for the one or more sub-networks **158**. The one or more sub-networks are typically interconnected and provide connectivity between one or more security servers, one or more roaming control servers. In some embodiments the security servers and roaming servers are organized hierarchically and a server can control associations and security on one or more sub-networks. Control or administration of the servers typically falls to the organization controlling the sub-networks managed. In some embodiments the roaming control servers and security servers can be distributed on the access points **160**. The use and management of hierarchical servers have already been discussed in detail.

What is claimed:

1. A system for securely accessing a wireless network, comprising:
a wireless mobile device configured to use wireless network protocols conforming to one or more of the IEEE 802.11 family of specifications; and
a program executing on the wireless mobile device, the program being configured to cause the mobile device to use an association control list to control communication with access points; the association control list comprising a plurality of BSSIDs; the program being further configured to update the association control list by communicating with a server.

2. The system of claim 1, wherein the association control list is specific to one or more network segments.

3. A system for securely accessing a wireless network, comprising:
a wireless mobile device; and
a program executing on the wireless mobile device, the program being configured to cause the mobile device to use an association control list to control communication with an access point, the association control list comprising digital data representing information concerning at least one access point and whether the wireless mobile unit should communicate with the at least one access point.

4. The system of claim 3 wherein the wireless network conforms to one or more of the IEEE 802.11 family of specifications.

5. The system of claim 3 wherein the wireless network conforms to one or more standards promulgated by The Bluetooth SIG, Inc.

6. The system of claim 3 wherein the wireless network is infrared.

7. The system of claim 3 wherein the association control list comprises a list of preferred access points with which the wireless mobile device will associate in preference to access points not on the list of preferred access points.

8. The method of claim 7 wherein the wireless mobile device searches for an access point on the list of preferred access point when the wireless mobile unit is not associated with an access point on the list of preferred access points.

9. The system of claim 3; further comprising a second association control list, the second association control list and the association control list forming at least a portion of an association control list hierarchy.

10. The system of claim 3, wherein the association control list is determined to reduce the cost of network access.

11. The system of claim 3, wherein the association control list is determined to increase network capacity and performance.

12. The system of claim 3, wherein the association control list comprises information identifying one or more access points with which the wireless mobile device is forbidden to associate.

13. The system of claim 3, wherein the association control list comprises information identifying one or more access points with which the wireless mobile device must exclusively associate.

14. The system of claim 3, wherein the association control list is updated by communicating with a server.

15. The system of claim 14, wherein the communication occurs over the wireless network.

16. The system of claim 14, wherein the communication occurs when the one or more mobile units are connected to a wired network.

17. The system of claim 15, wherein the client program authenticates an access point before updating the association control list via the access point.

18. The system of claim 14, wherein the client program authenticates the server before updating the association control list.

19. The system of claim 3, wherein the association control list is updated by communicating with a first server and is further updated by communicating with one or more additional servers.

20. The system of claim 19, wherein the first server and the one or more additional servers are hierarchically related.

21. The system of claim 19, wherein the precedence of association control policies applied the access control lists is determined with respect to the hierarchy.

22. The system of claim 3 wherein the association control list is updated by communicating with a first server, and a second association control list is updated by communicating with a second server, and the program is further configured to cause the mobile device to use the association control list and the second association control list to control communication with access points.

23. The system of claim 14, wherein the server automatically detects the presence of at least one new access point on at least one network segment and subsequently updates at least one association control list.

24. The system of claim 23, wherein the server adds the at least one access point with a known property or type to at least one association control lists.

25. The system of claim 23, wherein the server adds information identifying one or more access points of unknown type or properties to at least one association control list so as to forbid wireless devices using the at least one association control list from associating with the one or more access points of unknown type or properties.

26. The system of claim 23, wherein authorization of a network administrator is required to update an association control list.

27. The system of claim 3, wherein a server is used to facilitate the authentication of the access point by the mobile unit.

28. The system of claim 3, wherein the association control list is specific to one or more network segments.

29. A system for securely accessing a wireless network, comprising:
a wireless mobile device comprising a processor and memory; and
a program executing on the wireless mobile device, the program being configured to cause the wireless mobile device to associate with an access point and to send a request to a server for confirmation that the access point is authorized, the access point comprising a wireless device for communicating with wireless devices and a wired network interface for communicating via a wired network.

30. The system of claim 29, wherein the program is further configured to cause the wireless mobile device to cease association with the access point if the wireless mobile device does not receive confirmation that the access point is authorized.

31. The system of claim 29, wherein the wireless mobile device stores an identifier of the access point if the server does not confirm that the access point is authorized, and subsequently transmits the identifier to the server.

32. The system of claim 29 wherein the wireless network conforms to one or more of the IEEE 802.11 family of specifications.

33. The system of claim 29 wherein the wireless network conforms to one or more standards promulgated by The Bluetooth SIG, Inc.

34. The system of claim 29 wherein the wireless network is infrared.

35. The system of claim 31, wherein the server adds information identifying the access point to at least one association control list so as to forbid wireless devices using the at least one association control list from associating with the access point.

36. The system of claim 35, wherein authorization of a network administrator is required to update the list of access points.

37. A system for securely accessing a wireless network, comprising a server configured to receive a request to authenticate an access point from a wireless

mobile device, the server being further configured to determine whether the wireless mobile device is associated with the access point and whether the access point is authorized, and to provide a response to the wireless mobile device indicating whether the mobile device is authorized to continue association with the access point.

38. The system of claim 37, wherein the server is further configured to detect each association between the access point and the wireless mobile device and to disable communications between the access point and the wireless mobile device if no request to authenticate the access point is received within a predetermined interval.

39. The system of claim 37, wherein the server restricts the network access or network service privileges of the mobile device if the mobile device is not authorized.

40. A wireless communication security system, comprising:
a first wireless mobile device; and
a program executing on the first wireless mobile device, the program configured to cause the first wireless mobile device to use an association control list to control communication with other wireless mobile devices; the association control list comprising a plurality of identifiers, each identifier uniquely identifying a wireless mobile device.

41. The system of claim 40 wherein the wireless network conforms to one or more of the IEEE 802.11 family of specifications.

42. The system of claim 40 wherein the wireless network conforms to one or more standards promulgated by The Bluetooth SIG, Inc.

43. The system of claim 40 wherein the wireless network is infrared.

44. The system of claim 40, wherein the identifiers comprise IBSSIDs.

45. The system of claim 40 wherein one or more servers control the content of the association control list.

46. The system of claim 45 wherein a plurality of servers are organized in a hierarchy.

47. The system of claim 40 wherein the control list comprises information identifying one or more other mobile units with which a given mobile unit is forbidden to associate with.

48. The system of claim 40 wherein the control list comprises information identifying one or more other mobile units with which a given mobile unit must exclusively associate with.

49. A system for securely accessing a wireless network, comprising:
a wireless mobile device; and
a program executing on the wireless mobile device, the program being configured to cause the mobile device to use an association control list to control communication with access points and to update the association control list by communicating with a server.

50. The system of claim 3, wherein the program is further configured to cause the mobile device to use a user-configurable association control list to control communication with access points to the extent that the user-configurable association control does not conflict with the association control list.

51. The system of claim 3, wherein the program is further configured to cause the mobile device to select among a plurality of association control lists to control communication with access points based on an access point identifier transmitted by each access point.

52. A system for securely accessing a wireless network, comprising a server system comprising at least one server computer and at least one software program executing on the at least one server computer, the at least one server computer being operatively connected to a communications network, the system being configured to receive at least one access point identifier from a wireless mobile unit, the system being further configured to transmit to the

wireless mobile unit information concerning at least one access point and whether the mobile unit should communicate with the at least one access point.

53. The system of claim 52, wherein the server system is further configured to receive an identifier of the mobile unit.

54. The system of claim 52, wherein the server system is further configured to apply a criterion to determine at least a portion of the information.

55. The system of claim 54, wherein the criterion is inclusion of an identifier in an association control list.

56. The system of claim 55 wherein the wireless mobile unit complies with one or more of the IEEE 802.11 family of standards.

57. The system of claim 56 wherein the access point identifier comprises a BSSID.

58. The system of claim 55 wherein the wireless network conforms to one or more standards promulgated by The Bluetooth SIG, Inc.

59. The system of claim 52 wherein a plurality of servers are organized in a hierarchy.

60. The system of claim 55 wherein the association control list comprises information identifying one or more access points with which the unit is forbidden to associate with.

61. The system of claim 55 wherein the association control list comprises information identifying one or more access points with which the mobile unit must exclusively associate with.

62. The system of claim 55 wherein the wireless network is infrared.

63. A system for securely accessing a wireless network, comprising an access point comprising a wireless device for communicating with wireless devices and a wired network interface for communicating via a wired network, the access point configured to wirelessly transmit an association control list, the

association control list comprising digital data representing information concerning at least one access point and whether at least one wireless mobile unit should communicate with the at least one access point.

64. The system of claim 63 wherein the wireless network conforms to one or more of the IEEE 802.11 family of specifications.

65. The system of claim 64 where in the identifier comprises a BSSID.

66. The system of claim 63 wherein the wireless network conforms to one or more standards promulgated by The Bluetooth SIG, Inc.

67. The system of claim 63 wherein the wireless network is infrared.

68. The system of claim 63 wherein one or more servers control the content of the association control list.

69. The system of claim 68 wherein a plurality of servers are organized in a hierarchy.

70. The system of claim 63 wherein the association control list comprises information identifying one or more access points with which the unit is forbidden to associate with.

71. The system of claim 63 wherein the association control list comprises information identifying one or more access points with which the mobile unit must exclusively associate with.

72. The system of claim 63, wherein the access point is further configured to periodically broadcast the association control list.

73. The system of claim 63 wherein the association control list is transmitted with a beacon message of the access point.

74. A system for securely accessing a wireless network, comprising:
a wireless mobile unit comprising a processor and memory; and

a program executing on the wireless unit, the program configured to cause the wireless mobile unit to transmit to a server system a data structure comprising identifiers of access points within range of the wireless mobile units;

the program further configured to receive from the server system information concerning at least one access point and whether the mobile unit should communicate with the at least one access point.

75. A system for securely accessing a wireless network, comprising:

a wireless mobile unit comprising a processor and memory; and

a program executing on the wireless unit, the program configured to cause the wireless mobile unit to receive an association control list from an access point, the association control list comprising digital data representing information concerning at least one access point and whether the wireless mobile unit should communicate with the at least one access point.

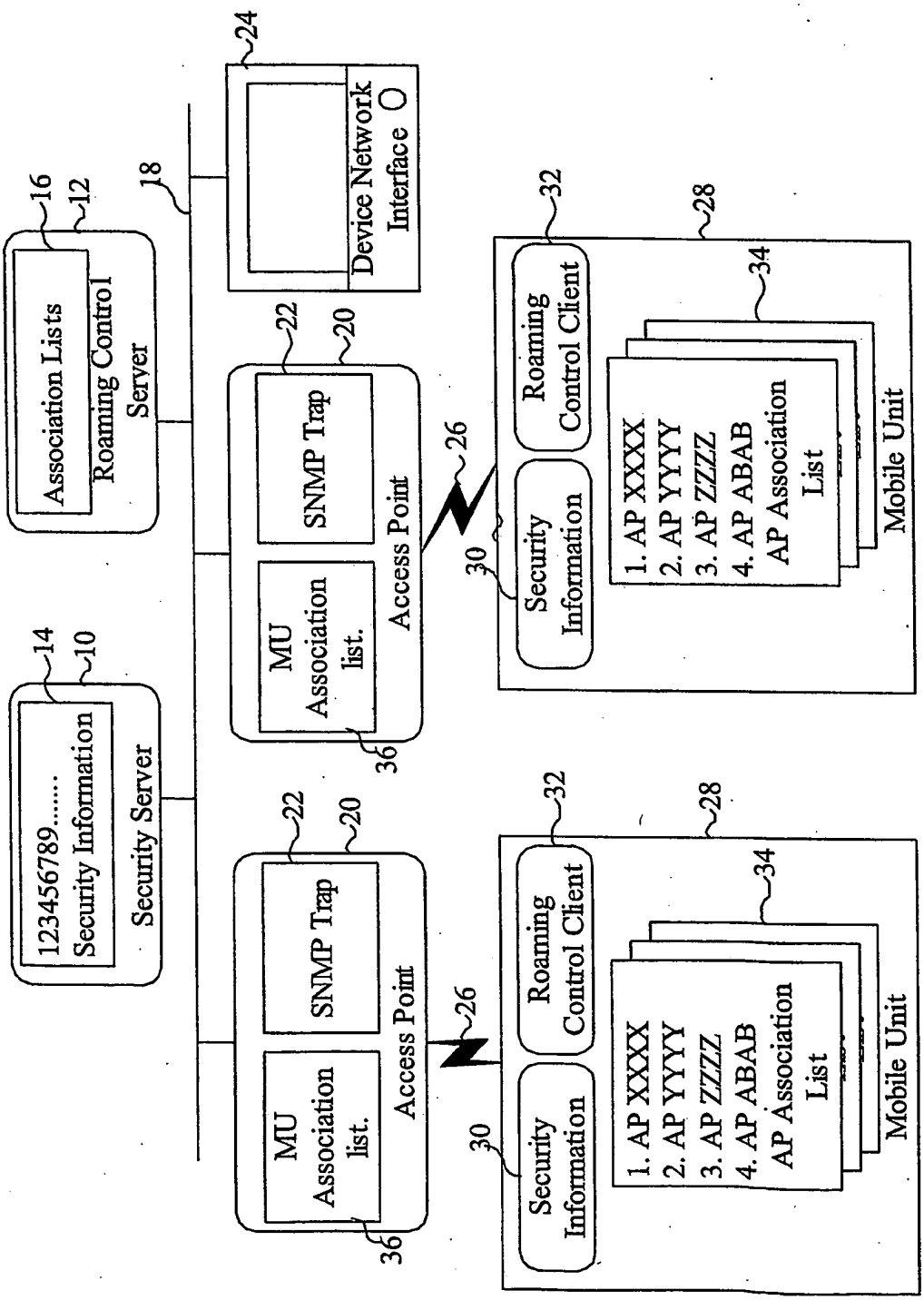


Figure 1. System Diagram

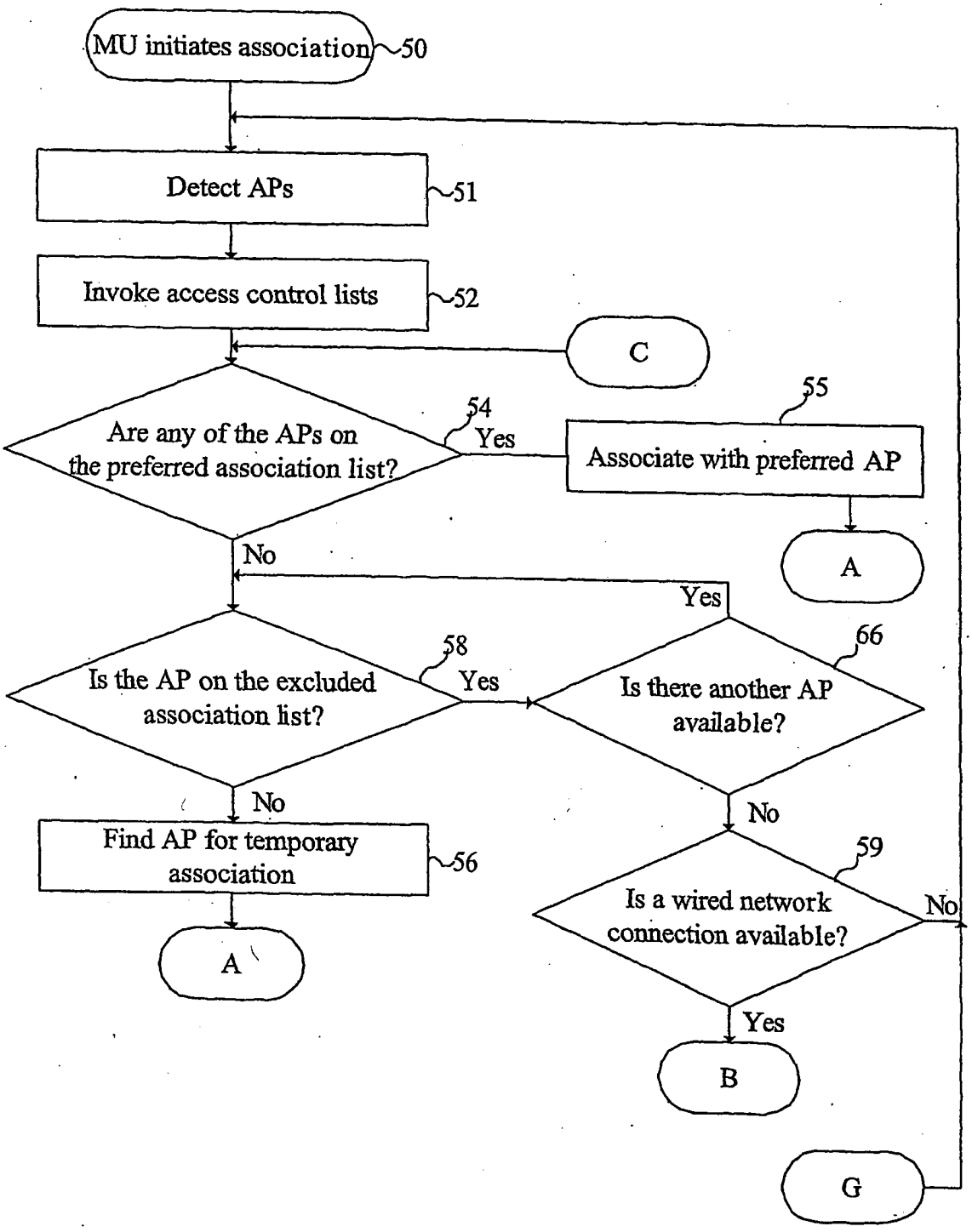


Figure 2A. Process Flow

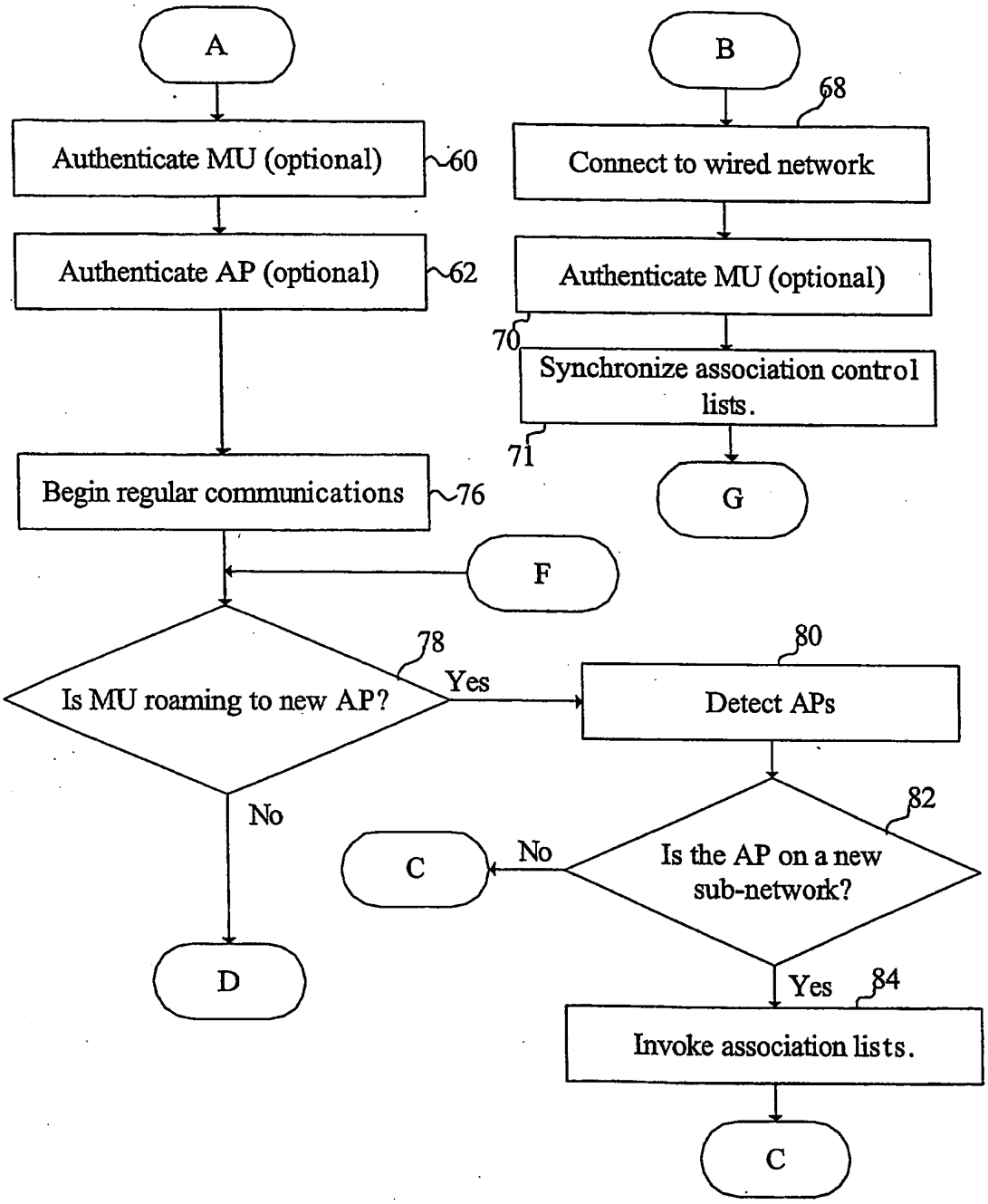


Figure 2B. Process Flow

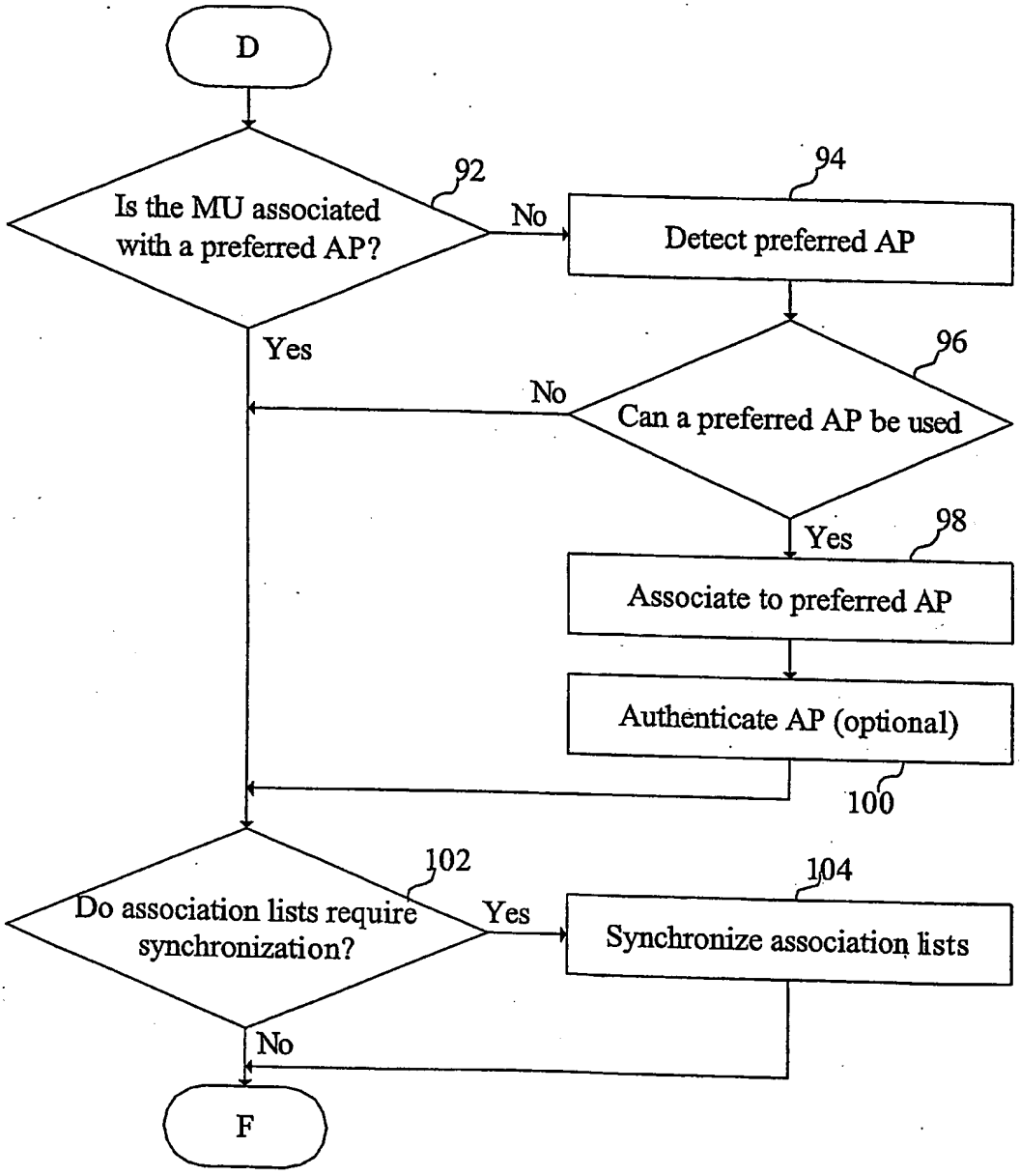


Figure 2C. Process Flow

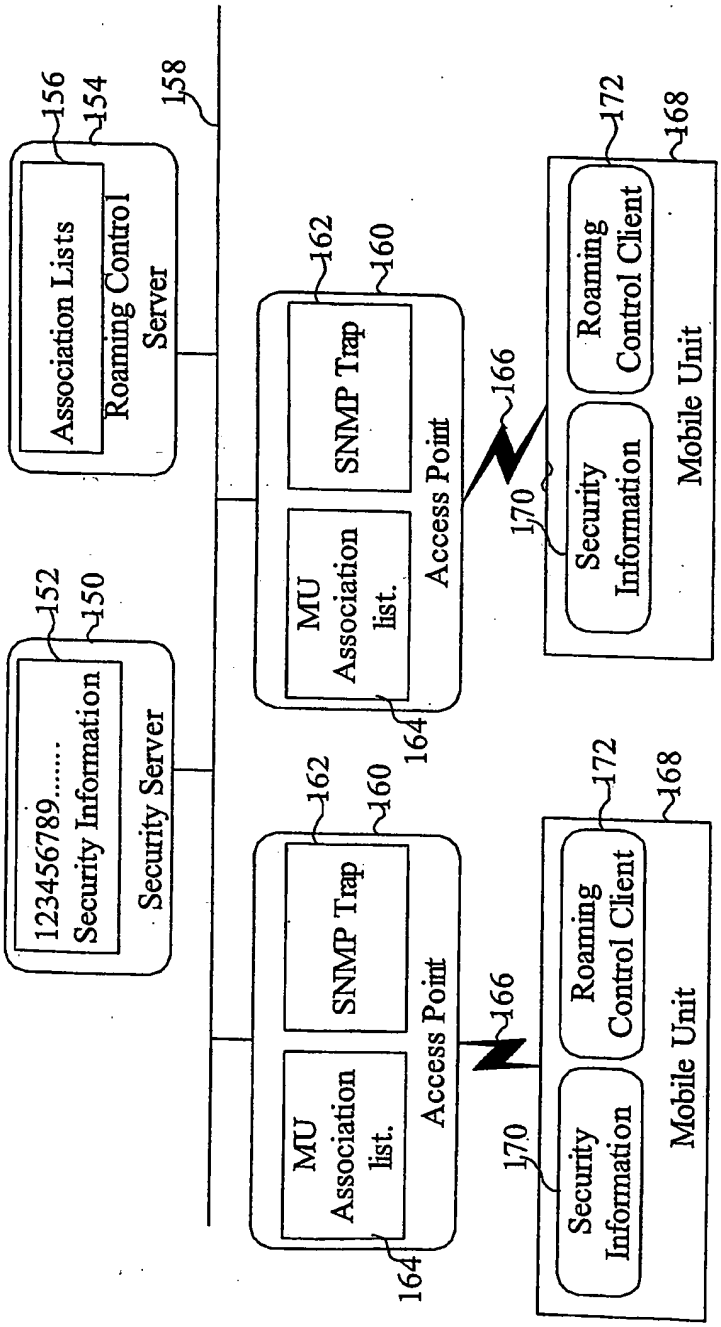


Figure 3. Alternative System Diagram

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 February 2004 (12.02.2004)

PCT

(10) International Publication Number
WO 2004/014024 A3

(51) International Patent Classification[7]: H04L 12/28

(21) International Application Number:
PCT/US2003/024180

(22) International Filing Date: 31 July 2003 (31.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/211,841 2 August 2002 (02.08.2002) US

(71) Applicant: **WAVELINK CORPORATION** [US/US]; 11332 NE 122nd Way, Suite 300, Kirkland, WA 98034 (US).

(72) Inventors: **WHELAN, Robert**; 545 Kirkland Avenue, Kirkland, WA 98033 (US). **VAN WAGENEN, Lamar**; 980 E. Diana Hills Way, Sandy, UT 84094 (US). **MORRIS, Roy**; 8812 NE 191st Place, Bothell, WA 98011 (US).

(74) Agents: **LEBOWITZ, Henry, C.** et al.; Pennie & Edmonds LLP, 1155 Avenue of the Americas, New York, NY 10036 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

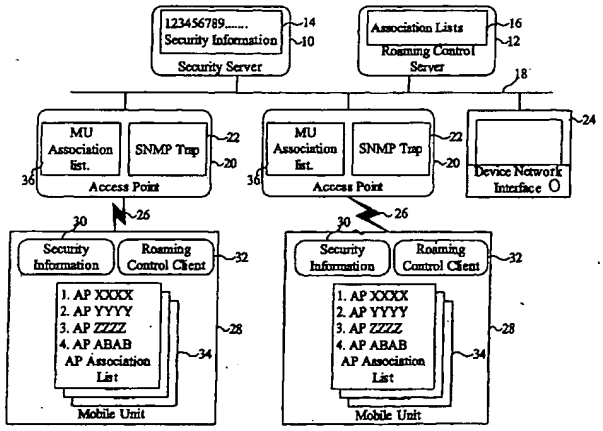
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
29 July 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: MANAGED ROAMING FOR WLANS



System Diagram

(57) Abstract: The present invention allows any number of mobile units to roam between a large numbers of sub-networks, each with a large number of access points (tens of thousands or more total access points), with minimal direct administration effort. A hierarchy of management servers may be used across the multiple sub-networks, which can be under the control of multiple entities. The invention provides the capability for the mobile units to authenticate the access points associated with, to ensure they are both authorized and managed. Peer-to-peer and ad hoc associations between mobile units are managed as welt. The invention may enforce a number of association policies such as, for example, forcing the mobile unit to only associate with access points or mobile units on a previously set mandatory association list, providing the mobile unit with a list of preferred access points to associate with, but allowing association with other access points, or providing the mobile unit with a excluded association list of access points or mobile units it is not to associate with.

WO 2004/014024 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/24180

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,Y	US 2003/117985 A1 (FUJII KAZUO ET AL) 26 June 2003 (2003-06-26) abstract; figures 1-6 page 4, paragraph 47 - paragraph 53	1,3,29, 37,40, 49,52, 63,74,75
Y	US 5 159 625 A (ZICKER ROBERT G) 27 October 1992 (1992-10-27) abstract; figures 9,14 column 16, line 32 - line 50	1,3,29, 37,40, 49,52, 63,74,75

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 May 2004	01/06/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Danielidis, S

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/24180

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	SALKINTZIS A K ET AL: "WLAN-GPRS INTEGRATION FOR NEXT-GENERATION MOBILE DATA NETWORKS" IEEE WIRELESS COMMUNICATIONS, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 9, no. 5, October 2002 (2002-10), pages 112-123, XP001132263 ISSN: 1070-9916 page 117, left-hand column, line 24 - line 40	1,3,29, 37,40, 49,52, 63,74,75
A	EP 1 081 895 A (INTEL CORP) 7 March 2001 (2001-03-07) abstract; figures 3a-3c column 5, line 39 - column 6, line 46	1,3,29, 37,40, 49,52, 63,74,75
A	US 5 838 730 A (CRIPPS PETER K) 17 November 1998 (1998-11-17) column 26, line 45 - column 27, line 66 column 30, line 38 - line 61	1,3,29, 37,40, 49,52, 63,74,75

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 03/24180

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003117985 A1	26-06-2003	JP 2003198571 A	11-07-2003
US 5159625 A	27-10-1992	NONE	
EP 1081895 A	07-03-2001	EP 1081895 A1	07-03-2001
US 5838730 A	17-11-1998	AU 7210894 A	17-01-1995
		WO 9501020 A1	05-01-1995
		US 5729680 A	17-03-1998
		US 5717688 A	10-02-1998
		US 5875186 A	23-02-1999